基于 IC 协议的分块加密方案及其应用 *

许盛伟 [1,2]，赵　海 [2]

(1. 北京电子科技学院 信息安全研究所，北京 100070; 2. 西安电子科技大学 通信工程学院，西安 710071)

摘　要：快递面单泄密问题在给个人带来安全隐患的同时，也制约着快递企业的快速发展。针对快递面单隐私保护进行了研究。将基于身份的加密体制（BF-IBE）、权限设计思想及二维码技术相结合，设计了一种分块加密方案，采用一种新的用户私钥分发协议（IC 协议）来解决密钥管理问题。将分块加密方案应用于快递隐私保护领域，设计了新型隐私面单与快递业务流程。结果分析表明，分块加密方案所采用的 IC 协议无须求逆运算，双线性对运算有效降低，便于密钥管理。在加解密效率上分块加密方案与 BF-IBE 相当，安全性基于椭圆曲线上的离散对数问题，应用于快递领域能有效保护用户隐私，可推广至其他有分块加密需求的领域。

关键词：快递面单；隐私保护；基于身份的加密；分块加密方案；密钥管理

中图分类号：TP309.7　　doi: 10.3969/j.issn.1001-3695.2017.11.0757

Block encryption scheme based on IC protocol and its application

Xu Shengwei[1, 2], Zhao Hai[2]

(1. *Research Institute of Information Security*, *Beijing Electronic Science & Technology Institute*, *Beijng* 100070, *China*; 2. *Communication Engineering Institute*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: The problem of leaking through express sheet brings security risks to individuals, but also restricts the rapid development of express enterprises. This paper studied the privacy protection of express sheet. By combining the identity based encryption system (BF-IBE) , the idea of authority design and the two-dimensional code technology, this paper designed a block encryption scheme. The scheme used a new private key distribution protocol (IC protocol) to solve the key management problem. This paper applied the block encryption scheme to the domain of express privacy protection, and designed a new privacy express sheet and express business process. The results show that the IC protocol used in the block encryption scheme needs no inverse operation, and the bilinear pairings can be effectively reduced and the key management can be carried out easily. The encryption and decryption efficiency of the block encryption scheme is similar to that of BF-IBE. Its security is based on the discrete logarithm problem on elliptic curves. It can be applied to express field, which can effectively protect the user's privacy. It is also suitable for other areas with block encryption requirements.

Key Words: express sheet; privacy protection; identity based encryption; block encryption scheme; key management

0　引言

随着近几年电商的高速发展，我国快递业发展进入快车道。《2016 年中国快递发展指数报告》指出：我国快递业务量规模居世界首位。预计 2017 年，我国快递业务量将达 423 亿件。规模巨大的业务量背后存在着泄露客户隐私信息的巨大隐患。《中国网民权益保护调查报告 2016》显示，超过 2.4 亿网购用户个人信息被泄露。其中，84%的用户遭受电话骚扰甚至是经济损失。客户隐私信息泄露问题不仅制约着快递业自身发展，也不利于快递实名制落地[1]。因此，加强个人信息安全保护显得极其重要。

快递业泄密主要有三个原因，一是快递企业内部人员私下贩卖客户信息，二是快递面单上的客户信息以明文形式显示，在快递流转的过程中极易被不法分子获取[2]。三是收件人签收快递后未经处理直接将快递面单丢弃，导致隐私信息泄露。本文主要针对后两者进行研究。

目前，国内纸质快递面单分为传统面单和隐私面单两类。传统面单将客户个人信息明文显示，在快递流转的过程中极易造成隐私信息泄露。对此，各大快递公司最近纷纷推出了隐私面单。不同于传统快递面单，隐私面单采用隐私保护技术对部分敏感信息进行隐藏，以保护客户隐私。

如表 1 所示，隐私面单虽然具有一定的保护作用，但还存

基金项目：国家“十二五”密码发展基金项目

作者简介：许盛伟（1976-），男，江西吉安人，副教授，博士，主要研究方向为信息安全、密码应用（xsw@besti.edu.cn）；赵海（1991-），男，山西晋城人，硕士研究生，主要研究方向为公钥密码体制应用.

在客户隐私信息保护不彻底问题。隐私面单目前还不完善，仍未普及。本文据此提出了一种基于 IC 协议的分块加密方案，并将其用于隐私面单设计，旨在弥补上述不足，提高隐私面单的安全性。

表 1　对隐私面单的信息保护技术分析

企业	特点	缺点
京东快递	收件人姓名、手机号的部分信息用符号（^_^）隐去	收件人地址信息明文显示
圆通快递	收件人姓名、手机号及详细地址的部分信息用*号隐去	物品名、寄件人信息全部明文显示
顺丰快递	寄件人姓名、地址、手机号完全隐藏，收件人保留姓名、地址，手机号中间四位用*号代替	收件人姓名、地址信息均明文显示
EMS 快递	使用 95013 安全号系统，将收件人联系方式用 95013 安全号替代	收件人地址、寄件人信息均明文显示

1　相关研究

1984 年，Shamir 提出了基于身份的加密体制 IBE(identity-based encryption)，这是一种公钥加密算法[3]。2001 年，Boneh 和 Franklin 设计出了第一个实用的加密方案 BF-IBE[4]。对比一般的公钥加密算法，在相同安全级别下 IBE 拥有更短的密钥。其公钥可以是任意唯一的字符串，如手机号码、邮箱帐号等，无须通过数字证书绑定用户公钥，避免了证书管理，降低了系统的复杂性[5]。

要想实际应用 IBE 加密体制，最关键的是要解决密钥托管和用户私钥安全分发问题[6]。针对该问题，目前的解决方案主要有三种：基于多可信机构的秘密共享门限方案[7, 8]、基于盲技术的方案[9]和基于分层结构的 HIBE 方案[11]。文献[7]利用可验证的(t,n)门限秘密共享方案，将用户私钥的共享问题转换为整数的秘密共享问题，减少了双线性对计算，降低了基于身份的加密方案中秘密泄露的风险。但至少 t 个 PKG 合谋可以得到用户临时私钥，通过文中私钥恢复公式仍可轻易得到用户真实私钥，用户私钥安全分发问题并未真正解决。文献[8]提出多 PKG 的门限 BF-FullIdent 改进方案以及多用户身份的门限 BF-FullIdent 改进方案，两个方案均基于多可信机构的秘密共享门限方案。通过将秘密共享于 n 个 PKG 间，分散了 PKG 过于集中的权力，提高了用户私钥的安全性，但同样存在至少 t 个 PKG 合谋欺骗问题，密钥托管问题仍未彻底解决。文献[9]基于盲技术解决了 PKG 和 PRA（私钥撤销机构）之间需要建立安全信道的问题，同时通过增加用户身份密钥解决了文献[10]中存在的 PKG 恶意攻击问题，但去盲化过程中的求逆运算及进行身份认证时大量使用的双线性对运算无疑增大了系统计算开销。基于分层结构的 HIBE 方案中，PKG 按分层树型结构分布。在分层结构中，任一节点的私钥泄露不会影响上层 PKG 及其他 PKG 的安全。文献[11]提出一种层次式基于身份加密系统 T-HIBE，系统引入私钥用户盲因子、用户私钥编号因子和 PKG 私钥编号因子技术，通过层次化 PKG 和多个密钥隐私机构 KPA 共同为用户产生私钥，虽然解决了 HIBE 体制中的密钥托管和私钥安全传输问题，但系统构成复杂，用户为了进行身份认证并得到用户私钥，需要和 n 个 KPA 通信，而且去遮蔽因子计算降低了系统效率，当用户数量很大时，系统负担过重。文献[12]引入了盲化技术和身份证书概念，能同时较好地解决用户私钥安全分发与密钥托管问题。本文提出一种新的用户私钥分发协议（identity certificate），下文中简称 IC 协议。与文献[12]协议相比，该协议在保持系统简洁性的同时，降低了运算量，且便于用户更换密钥。

2　方案

2.1　IC 协议

IC 协议与文献[12]中的用户私钥分发协议类似，都基于多可信机构的秘密共享门限方案。IC 协议模型主要由可信认证中心（TA）、n 个私钥生成器（PKG）和客户端组成，如下图所示。

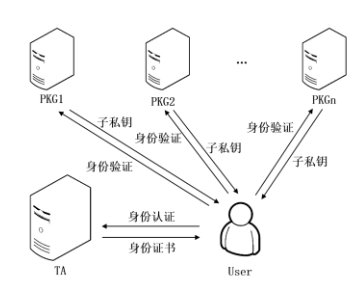


图 1　IC 协议模型

IC 协议流程由系统初始化、用户身份认证、用户私钥分发这三部分组成。

1）系统初始化

(a) 系统产生如下参数：q 是大素数，G 是由椭圆曲线上的点构成的阶为 q 的加法循环群，P 是群 G 的生成元，双线性映射 $e: G\times G\rightarrow G_T$ （G_T 是乘法群）。

(b) TA 随机选择 $s_0\in Z_q^*$ 作为签名私钥，并计算 TA 的公钥 $P_0=s_0P$，s_0 保密。

(c) 系统随机选择 $s\in Z_q^*$ 作为主密钥，通过 Shamir 门限方案将 s 共享于 n 个 PKG_i 间，各 PKG_i 拥有自己的私钥秘密份额 $s_i(1\le i\le n)$，任意 t 个以上的 PKG 合作可以得到主密钥 s，令 $P_{pub}=sP_0$。

(d)选择两个 Hash 函数 $H_1:\{0,1\}^*\rightarrow G$，$H_2: G_T\rightarrow\{0,1\}^n$。

(e) 公开参数 $<q,G,G_T,e,P,P_0,P_{pub},H_1,H_2>$。

2)用户身份认证

(a) 用户 User 的身份标志为 ID，User 随机选取自己的主密钥 $x\in Z_q^*$，计算相应的公钥 $Q_x=xQ_{ID}$，其中 $Q_{ID}=H_1(ID)$。

(b) User 发送 Q_x 和 Q_{ID} 给 TA，TA 确认用户身份后计算 User 身份证书 $IC=s_0Q_{ID}$，并发送 IC 给 User。

(c) User 计算用户签名 $Sig_x=xP$，发送身份验证信息 $AI=<Sig_x,IC,Q_x>$ 给 $PKG_i(i=1,2,\cdots,t)$，PKG_i 验证等式 $e(Sig_x,IC)=e(P_0,Q_x)$ 是否成立，成立则身份验证通过，否则 PKG_i 拒绝分发私钥。

3)用户私钥分发

(a) PKG_i 生成用户子私钥 $s_iIC(1\le i\le n)$，并将子私钥通过公共信道发送给 User。

(b)User 用对应的拉格朗日系数乘以各子私钥之后再相加得到 sIC，最后计算出用户私钥 $d_{ID}=xsIC=xss_0Q_{ID}$。

2.2 分块加密方案

基于 IC 协议，本文提出一种分块加密方案，该方案的模型如图 2 所示。

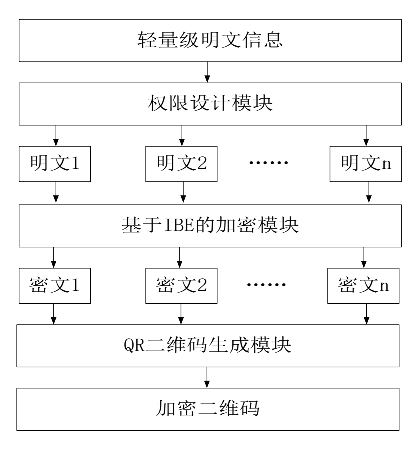


图 2 分块加密模型

分块加密模型由权限设计模块、加密模块、二维码生成模块三部分组成。权限设计模块对各级角色进行划分并对明文进行分块处理。加密模块基于 IBE 加密体制，用各角色公钥对明文块分别进行加密。QR 二维码又叫快速响应二维码，具有存储容量大、成本低、便于读取、容错能力强、译码可靠性高等优点[2]，在各个领域应用广泛[13]。引入二维码模块是为了提高方案整体效率，特别地，将二维码作为加密信息载体，应用在快递面单上不仅可以保护用户隐私，还提高了快递业务效率。

具体的分块加密方案如下：

a)根据需求进行权限设计，确定 n 级角色 R_1，R_2，……，R_n。

b)按照 IC 协议依次完成系统初始化、n 级角色身份认证和私钥分发。

c)依据权限设计，将轻量级明文信息 m 分成 n 个明文块 m_1，m_2，……，m_n。

d)User 获取 n 级角色的公钥 Q_{x_i}，随机选取 $r_i\in Z_q^*$，计算各密文块 $c_i=<U_i,V_i>$，其中 $U_i=r_iP$，$V_i=m_i\oplus H_2(e(Q_{x_i},P_{pub})^{r_i})$ $(1\le i<n)$。

e)密文 c（$c=c_1\|c_2\|\cdots\|c_n$，“$\|$”为连接符）通过二维码生成模块生成加密二维码 Qr，将 Qr 发送给各级角色。

f) R_i $(1\le i<n)$ 收到二维码 Qr 后，扫描 Qr 得到对应密文块 c_i。检查 $U_i\in G$ 是否成立，不成立则拒绝该密文。成立则用自己的私钥 d_{ID_i} 解密，计算得到明文 $m_i=V_i\oplus H_2(e(d_{ID_i},U_i))$。

3 方案在快递中的应用

3.1 隐私面单设计

首先，分析快递中的业务需求。快递面单上的信息可分为三类：寄件人信息，收件人信息和物品信息。寄、收件人信息包括：姓名、联系方式、目的地址（省市区/县）及详细地址，物品信息主要是物品名称。在实际的快递业务流程中，一般包含五级角色，各级角色为完成自己相应的操作需要从快递面单上获取某些信息，具体情况如表 2 所示。

表 2 快递中各级角色所需信息及相关操作

角色	操作	所需信息
寄件员	寄件	\
揽件员	收件	\
配件员	分拣、中转	收件人目的地址
派件员	派件	收件人详细地址、联系方式
收件人	签收	收件人姓名、物品名称

事实上，快递面单上的信息除了目的地址外，均为需要保护的隐私信息。由表 2 知，这些隐私信息只需对特定角色公开，而对其他角色应当保密。按照这种需求将明文分为 4 块，用 4 级角色公钥对各明文块进行加密。具体的快递隐私信息权限设计如表 3 所示。

表 3 快递隐私信息权限设计

隐私信息	加密公钥
收件人姓名、物品名	收件人公钥 Key_R
收件人详细地址及联系方式	派件员公钥 Key_D
寄件人姓名、物品名	寄件人公钥 Key_S
寄件人详细地址及联系方式	揽件员公钥 Key_C

注：寄件人信息在快递被退回时可用到。

针对现有隐私面单的不足，结合上述分析，将所提分块加密方案用于快递隐私信息保护，设计了如图 3 所示的新型隐私面单。



图 3 分块加密模型

相对于目前市面上的隐私面单对用户信息半隐半露，该新型隐私面单依据分块加密方案对所有的用户隐私信息进行了加密处理，做到了全方位保护。仅保留寄、收件人的目的地址（省市区/县）用于快递分拣、中转，保留快递单号用于后台同步物流信息。

3.2 快递业务流程设计

新的快递业务流程图设计如图 4 所示。

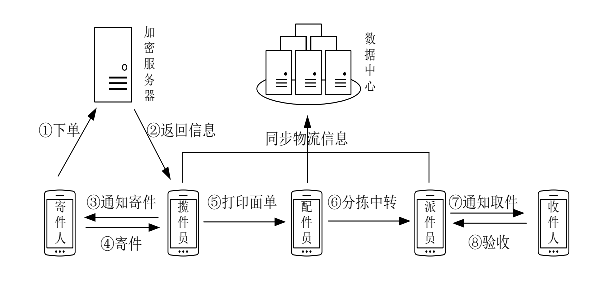


图 4 快递业务流程图

基于分块加密方案的具体快递业务流程如下：

a) 寄件人用快递专用 App 在线下单。

b) 加密服务器基于分块加密方案对订单信息进行处理：寄件人姓名、所寄物品名称用寄件人公钥加密，寄件人详细地址及联系方式用揽件员公钥加密；收件人姓名、所寄物品名称用收件人公钥加密，收件人详细地址及联系方式用派件员公钥加密。然后，加密服务器将密文及寄、收件人目的地址返回给揽件员。

c) 揽件员解密密文获知寄件人详细地址和联系方式，并联系寄件人寄件。

d) 揽件员收件后，使用 App 生成快递隐私面单电子版，并使用便携打印设备打印张贴到快递包裹上，同时将物流信息同步至数据中心。

e) 配件员根据收件人目的地址对快递进行分拣、中转，同时将物流信息同步至数据中心。

f) 派件阶段，派件员利用 App 扫描隐私面单上的收件人加密二维码，获知收件人详细地址及联系方式，联系收件人取件。

g) 收件人扫描收件人加密二维码，获知本人姓名及物品名，验证后签收。

h) 收件人签收后，派件员将物流信息同步至数据中心。

传统纸质快递面单的收、寄件人信息需要手动填写，效率较低[14]，且客户隐私信息泄露的风险很大。电子面单则在客户端在线填写收、寄件人信息，借助二维码进一步提升了效率。但客户信息明文存储在二维码中，导致隐私泄露问题依然存在。本文将新型隐私面单引入快递业务流程后，业务流程实质可以分为两部分：快递分拣、中转流程以及揽件、派件阶段的加解密流程。隐私面单保留了目的地址及快递单号条形码。快递公司员工可根据目的地址分拣、中转快递，同时使用巴枪扫描条形码以完成后台物流信息更新。这一阶段对快递效率影响不大。加密过程在揽件员上门收件前就已经完成，真正影响快递效率的只有各角色所对应的解密操作。而由 4.2 节加解密效率分析可知，解密耗时在几十毫秒量级，实际应用中会牺牲一定的便捷性。但为了有效保护客户隐私信息，这种代价是值得的。

4 方案分析

下面对本方案进行性能分析，包括正确性、加解密效率、安全性分析及 IC 协议分析。

4.1 正确性

证明方案的正确性只需证明加密信息经解密可恢复为相应明文即可。设角色 R_i 收到密文 $c_i = \langle U_i, V_i \rangle$ 后用私钥 d_{ID_i} 解密，将 $V_i = m_i \oplus H_2(e(Q_{x_i}, P_{pub})^{r_i})$，$d_{ID_i} = x_i ss_0 Q_{ID}$，$U_i = r_i P$ 带入下式，根据双线性映射的双线性性可知：

$$V_i \oplus H_2(e(d_{ID_i}, U_i))$$

$$= m_i \oplus H_2(e(Q_{x_i}, P_{pub})^{r_i}) \oplus H_2(e(x_i ss_0 Q_{ID}, r_i P))$$

$$= m_i \oplus H_2(e(Q_{ID_i}, P_{pub})^{x_i r_i}) \oplus H_2(e(Q_{ID_i}, ss_0 P)^{x_i r_i})$$

$$= m_i$$

由此证明了方案的正确性。

4.2 加解密效率

本文分块加密方案基于 BF-IBE 加密方案，而分块加密方案的提出是为了解决快递面单隐私信息泄露问题.。故用分块加密方案与 BF-IBE 方案模拟实际快递业务中的加解密流程，对两种方案进行实际效率比对实验。

在分块加密方案中取 n=4(模拟快递流程中的四级角色)，对收、寄件人隐私信息分块后用对应的四级角色公私钥进行加解密，而 BF-IBE 方案因为没有分块概念，不妨采用揽件员和派件员公私钥分别对收、寄件人隐私信息进行加解密。

实验环境：集成开发环境为 Android Studio（导入 JPBC 库实现双线性对的计算），程序用 Java 语言实现。将程序打包后生成的 APK 文件在主频 2GHz、内存 2G 的 Android 手机上运行。在该实验条件下，两种方案对同样的收、寄件人信息进行加解密。因生成、扫描二维码的速度极快，这里忽略不计，只统计加解密的耗时。其中加密耗时为加密收、寄件人隐私信息的耗时总和，解密耗时为解密收件人隐私信息的耗时，重复实验 100 次取均值，结果如表 4。

表 4 两种方案的加解密效率对比

方案	加密平均耗时/ms	解密平均耗时/ms
BF-IBE 方案	249.2	57.5
分块加密方案	296.5	62.3

实验结果表明，当 n 为 4 时，分块加密方案与 BF-IBE 方案的加密效率比约为 1:1.2，解密效率比约为 1:1.1，相差不大。

4.3 安全性

分块加密方案的安全性主要取决于用户私钥的安全性。本

方案的用户私钥由可信认证中心（TA）、私钥生成器（PKG）和用户三方共同生成。若 TA 被非法控制，攻击者只能获取用户信息 Q_x 和 s_0。因为得不到系统主密钥 s，故攻击者无法最终得到用户私钥。若至少 t 个 PKG 合谋，也只能得到 sIC，因为没有用户主私钥 x，所以也无法得到用户私钥。只要 TA 与 PKG 不同时被攻击者控制，则可以保证用户私钥不被攻击者获取。

此外，因为本方案所有信息均在公共信道传输，攻击者可以轻易截获 PKG 发给用户的 t 个以上的子私钥信息，经计算可得 ss_0Q_{ID}。若想进一步得到用户私钥 $d_{ID}(xss_0Q_{ID})$，则只能从 $Sig_x(xP)$ 或 $Q_x(xQ_{ID})$ 计算得到 x，但这是一个椭圆曲线上的离散对数问题。攻击者也可以截获 TA 发送给用户的身份证书 $IC(s_0Q_{ID})$，为了得到用户私钥，只能从 $Sig_x(xP)$ 及 $P_{pub}(sP_0)$ 计算得到 x 和 s。但这两个问题均为椭圆曲线上的离散对数问题。当然，攻击者还可以获取用户公钥 $Q_x(xQ_{ID})$。为了得到用户私钥，只能从 $P_{pub}(sP_0)$ 及 $P_0 = s_0P$ 得到 s 和 s_0，这两个问题依然属于椭圆曲线上的离散对数问题。

由上述分析可知，本文提出的分块加密方案的安全性实质上基于椭圆曲线上的离散对数问题（ECDLP），即通过已知信息 $P, rP \in G$ 计算出整数 r 是一个困难问题。该问题的难解性决定了本方案的安全性。

已经证明[4]，BF-IBE 方案在随机预言机模型下是选择密文安全的。本文给出的方案没有改变 BF-IBE 的原加密算法，只是将 BF-IBE 方案扩展到分块加密上，并不会导致安全性降低。

4.4 IC 协议分析

本协议与文献[12]相比，保留了原协议在私钥分发及密钥托管上的优势，同时减少了计算量，可灵活更换用户密钥，提高了协议效率。

1) 私钥安全传输问题

在 AIC 协议中采用盲技术来加密用户子私钥，用户通过求逆运算得到用户私钥，解决了 PKG 分发用户私钥时需要建立安全信道的问题。由 IC 协议的步骤 3 可知，用户私钥由用户主密钥 x、系统主密钥 s 及用户身份证书 IC 共同组成。当 PKG_i 生成的用户子私钥 s_iIC 在公共信道上传输时，即使敌手截获 t 个以上的用户私钥信息，也只能得到 sIC，因为敌手没有用户主私钥 x，所以无法得到用户私钥。由此可知，IC 协议不仅解决了用户私钥安全传输问题，还避免了求逆运算，降低了运算量。

2) 密钥托管问题

为了解决 IBE 固有的密钥托管问题，IC 协议建立了一种多方密钥托管机制。当政府机构在特殊情况下需要解密用户信息，或者用户私钥丢失或损坏时，可通过 TA 获取用户信息 Q_x 和 s_0，通过至少 t 个 PKG 获取系统主密钥 s，即可得到用户私钥 $(d_{ID} = ss_0Q_x)$。相反，t 个以上的 PKG 合谋只能得到系统主密钥 s，因为得不到 TA 签名私钥 s_0，所以 PKG 合谋无法获取用户私钥。

3) 效率对比

表 5　IC 协议与 AIC 协议的运算量对比

运算类型	AIC 协议	IC 协议
乘法运算	t + 7	t + 6
求逆运算	1	0
Hash 运算	1	1
对运算	4t	2t
合计	5t + 9	3t + 7

由表 5 可知，本文协议与文献[12]中协议相比，乘法运算减少一次，无须求逆运算，双线性对运算减少了一半。

4)密钥更换

根据文献[6]，IBE 中用户私钥更换需要用户在选择公钥的时候加上时间段字符串作为公钥的一部分，私钥超过有效期就不再使用。但这种策略不够灵活，当有效期内发生用户私钥泄露问题时，私钥更换难以进行。文献[12]中并未解决密钥更换问题，且从其用户私钥的构成来看（$d_{ID} = ss_0Q_{ID}$），用户私钥完全依赖于系统参数，更换困难。而 IC 协议中引入用户主密钥 x 作为用户私钥的一部分，用户只需更新用户主私钥 x 与公钥 Q_x 即可完成密钥更新。

4.5 实际密钥管理问题

实际应用中密钥管理包括密钥生成、密钥分发、密钥存储和密钥更新等。本文方案通过 PKG 服务器和 TA 服务器来共同完成密钥管理。由一台根 PKG 服务器来完成系统参数初始化，并将系统主密钥 s 共享于 n 台子 PKG 服务器间。TA 服务器及 PKG 服务器可以由快递公司的可信服务器来担任。

1）密钥生成与分发

用户在手机 App 上用身份标志 ID 完成注册，App 提交用户信息 Q_x 和 Q_{ID} 给 TA 服务器。TA 服务器确认用户身份后，将 Q_x 和 Q_{ID} 存储在自身公钥数据库（PKDB）中，并向用户 App 发送身份证书 IC。用户 App 收到身份证书后计算用户签名 Sig_x，并发送身份验证信息给 $PKG_i(i = 1, 2, \cdots, t)$ 服务器。PKG_i 服务器验证用户身份后通过公共信道向用户 App 发送子私钥，最后用户 App 经计算得到用户私钥 d_{ID}。

2）密钥存储

用户获取自己的私钥后，将私钥存储于手机本地数据库文件 key.db 中。用户的公钥存储于 TA 服务器的公钥数据库（PKDB）中。

3）密钥更新

当用户需要更新密钥时，向 TA 服务器发起申请并提交新的公钥 $Q_{x'}$。TA 服务器根据用户 ID 查询公钥数据库，得到该用户的 Q_x 和 Q_{ID}。TA 服务器随机选取 $r \in Z_q^*$，计算 rP 并将其发送给用户。用户计算 xrP 并发送给 TA 服务器，TA 服务器验证 $e(xrP, s_0Q_{ID}) = e(s_0rP, Q_x)$ 是否成立。若成立则在公钥数据库中更新 Q_x 为 $Q_{x'}$，并发送密钥更新成功的消息给用户。用户得知密钥更新后，将主密钥 x 更新为 x'。

4.6 方案对比

文献[15]针对快递员递送包裹这个环节可能存在的隐私泄露问题，提出一种变型的重新平衡-RSA 方案，将其应用于客户隐私信息数据加密，一定程度上保护了快递隐私信息。但将客户姓名、手机号加密，只暴露家庭住址给派件员，存在派件员在派件前无法联系客户的问题。文章也未说明如何解决快递流程的其他环节同客户隐私信息保护的矛盾。此外，不使用快递面单，无疑增大了其他环节匹配包裹所消耗的时间。文献[16]基于 DES 和 RSA 加解密技术，设计了一种电子面单，可在整个快递流程中有效保护客户隐私信息，但派件员权限过大，可解密获取客户的全部隐私信息，存在泄密的潜在隐患。另外，RSA 必须借助复杂的 CA 系统来进行密钥管理，需要占用较多资源。文献[17]提出了基于二维码技术的个人信息隐私保护物流系统 LIPPS，有效解决了物流信息加密与物流业务流程的矛盾，但验证云平台实时生成密钥对时间要求很高，云平台与移动终端进行密钥传输需要额外借助安全信道，且收件时终端采用 RSA 来加密数据导致还是无法规避使用 CA 的问题。文献[18]结合二维码技术与传统公钥加密技术，设计了一种物流业个人信息隐私保护方案，实现了全方位、全流程的个人信息隐私保护。文中派件员可解密的客户隐私信息包括姓名、手机号与地址，但解密后的姓名信息只是做了隐藏，并未有效利用。同时方案基于传统公钥加密体制，还是需要利用 CA 来进行密钥管理。本文提出一种分块加密方案，可有效解决以上方案存在的问题。基于该方案设计了一种快递隐私面单，面单上仅留目的地址用于快递中转，其他客户隐私信息根据权限设计，经加密形成加密二维码。其中收件人姓名用收件人公钥进行加密，用于快递签收阶段的身份验证。密钥管理基于 IC 协议，无须 CA，简单方便，且密钥传输无须借助安全信道。

5 结束语

本文设计的 IC 协议可有效解决 IBE 体制存在的用户私钥安全分发和密钥托管问题，且与 AIC 协议相比，IC 协议的乘法运算减少一次，无须求逆运算，双线性对运算减少一半，密钥更换灵活方便。在 IC 协议的基础上，提出一个分块加密方案。分块加密方案可有效保护用户隐私，加解密效率与 BF-IBE 方案相当，安全性基于椭圆曲线上的离散对数问题。基于该方案设计了一种新型快递隐私面单，最大程度地保护了用户隐私信息，弥补了目前各隐私面单存在的不足。将新型隐私面单应用到新的快递业务流程中，解决了用户信息加密与快递业务流程间的矛盾，可推广至外卖清单隐私保护等有分块加密需求的其他领域。

参考文献：

[1] 廖欣，周翼. 论快递服务与网购个人信息保护 [J]. 物流科技, 2014 (1): 114-115.
[2] 严璞. 基于手机二维码的物流管理信息系统设计与实现 [D]. 武汉：华中科技大学, 2011.
[3] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proc of Crypto. [S. l.] : Springer-Verlag, 1984: 47-53.
[4] Boneh D, Franklin M. Identity based encryption from the Weil pairing [C]// LNCS vol 2139. 2001: 213-229.
[5] 曾梦岐，卿昱，谭平璋. 基于身份的加密体制研究综述 [J]. 计算机应用研究, 2010, 27 (1): 27-31.
[6] 李玉欢. 基于身份加密体制密钥管理研究与应用 [D]. 成都：电子科技大学, 2016.
[7] 封化民，孙轶茹，孙莹. 基于身份认证加密的私钥共享方案及其应用 [J]. 计算机应用研究, 2014, 31 (5): 1507-1510.
[8] 慈云飞，李凤华，史国振，等. 基于双线性配对构造的身份加密体制 [J]. 北京电子科技学院学报, 2015, 23 (2): 34-39.
[9] 侍伟敏. 基于 mIBE 的密钥托管和身份撤销方案 [J]. 华中科技大学学报：自然科学版, 2011 (5): 76-78.
[10] Oh J H, Lee K K, Moon S J. How to solve key escrow and identity revocation in identity-based encryption schemes [C]// LNCS vol 3808. Berlin: Springer-Verlag, 2005: 290-303.
[11] 王小峰，陈培鑫，周寰，等. 一种可信安全的层次式基于身份加密系统 [J]. 电子学报, 2016, 44 (7): 1521-1529.
[12] 侍伟敏. 基于 AIC 的 IBE 私钥分发协议 [J]. 北京邮电大学学报, 2008, 31 (4): 74-76.
[13] 方文和，李国和，吴卫江，等. 面向 Android 的 RSA 算法优化与二维码加密防伪系统设计 [J]. 计算机科学, 2017, (1): 176-181.
[14] 杜晨杰，张少中，姚英彪. 一种基于加密二维码标签的新型快递管理系统 [J]. 浙江万里学院学报, 2017, 30 (3): 19-25.
[15] 韦茜，王晨，李星毅. RSA 算法的快递信息隐私保护应用 [J]. 电子技术应用, 2014, 40 (7): 58-60.
[16] 周春樵，朱思征，王山山，等. 快递信息管理系统中隐私保护研究 [J]. 物流工程与管理, 2015, 37 (12) .
[17] 张新文，李华康，杨一涛，等. 基于二维码技术的个人信息隐私保护物流系统 [J]. 计算机应用研究, 2016, 33 (11): 3455-3459.
[18] 胡卫，吴邱涵，顾晨阳. 基于二维码的物流业个人信息隐私保护方案设计 [J]. 通信技术, 2017, 50 (9) .